VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

GDPR 2016/679

"MINISTERO DELL'ISTRUZIONE"
Istituto Comprensivo "Aldo Moro"
Via Fossadelli, 25 – 25031 Capriolo (Bs)
Tel: 030 736096
Email: bsic83300l@pec.istruzione.it – bsic83300l@istruzione.it
SITO WEB – http:// www.iccapriolo.edu.it

CONSEGNA SDG	23/02/2022	FIRMA TT/RSG:	
DATA REVISIONE	**NOTE**	**FIRMA AUDITOR**	**FIRMA RSG e/o DS**
08/09/2022	Inviate informative; istruzioni AgID, per maggiori info vedere verbale di audit	AUD003 dott. Lorenzo Casali	

VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

La DPIA, acronimo di Data Protection Impact Assessment, è una valutazione preliminare,eseguita dal titolare del trattamento dei dati personali, relativa agli impatti a cui andrebbe incontro un trattamento laddove dovessero essere violate le misure di protezione dei dati.

In linea con l'approccio basato sul rischio adottato dal regolamento generale sulla protezione dei dati, non è obbligatorio svolgere una valutazione d'impatto sulla protezione dei dati per ciascun trattamento; è necessario realizzare una valutazione d'impatto sulla protezione dei dati soltanto quando la tipologia di trattamento "può presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (articolo 35 del Regolamento 2016/679).

OBBLIGO DPIA

Ai sensi dell'articolo 35, paragrafo 3 del Regolamento 2016/679 la valutazione è stata effettuata nei casi in cui un trattamento può presentare rischi elevati, ossia quando:

a. una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sullaquale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
b. il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10;
c. la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

CRITERI DA CONSIDERARE PER OBBLIGO DPIA

Nel percorso di analisi sono stati presi in considerazione i seguenti 9 criteri:

1. Valutazione o assegnazione di un punteggio
2. Processo decisionale automatizzato che ha effetto giuridico o incide in modoanalogo significativamente
3. Monitoraggio sistematico
4. Dati sensibili o aventi carattere altamente personale
5. Trattamento di dati su larga scala
6. Creazione di corrispondenze o combinazione di insieme di dati
7. Dati relativi ad interessati vulnerabili
8. Uso innovativo o applicazione di nuove soluzioni tecnologiche
9. Trattamento che impedisce agli interessati di esercitare un diritto o di avvalersidi un servizio o di un contratto

Nel caso in cui un'attività di trattamento dati soddisfa due o più criteri viene eseguita lavalutazione d'impatto sulla protezione dei dati.

VALUTAZIONE PROBABILITA'

IDENTIFICAZIONE DEI TRATTAMENTI

Il primo step consiste nel censire tutte le attività di trattamento di dati personali specificandone:

- dati identificativi (Sede, struttura, funzioni),
- finalità,
- tipologia di dati personali trattati,
- categorie di interessati,
- destinatari,
- modalità di elaborazione dati (cartacea, elettronica, mista),
- termine cancellazione dati,
- eventuale trasferimento paesi terzi,
- misure di sicurezza.

VALUTAZIONE DEL RISCHIO E INDIVIDUAZIONE CRITERI PER DPIA

Un rischio è uno scenario che descrive un evento e le sue conseguenze, stimato intermini di gravità e probabilità. L'entità dei rischi viene ricavata assegnando un opportuno valore alla **probabilità di accadimento (P)** e ai **danni** di tale evento **(D)**. Dalla combinazione di tali grandezze si ricava la matrice di rischio la cui entità è data dalla relazione:

$$LR = P \times D$$

LR = LIVELLO DI RISCHIO
P = PROBABILITÀ DI ACCADIMENTO
D = DANNO

	IMPATTO	LIVELLO	DESCRIZIONE
VALUTAZIONE DELL'IMPATTO/ GRAVITÀ	**4**	**GRAVE**	Individui che possono avere conseguenze significative, o addirittura irreversibili, che non possono superare (incapacità di lavorare, disturbi psicologici o fisici a lungo termine, morte, ecc.).
	3	**SIGNIFICATIVO**	Gli individui possono incontrare conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (perdita significativa di denaro, inserimento di liste nere da parte di istituti finanziari, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, peggioramento della salute, ecc.).
	2	**MODERATO**	Gli interessati possono incontrare significativi disagi, che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, rifiuto di accesso ai servizi, paura, mancanza di comprensione, stress, disturbi fisici minori, ecc.).
	1	**TRASCURABILE**	Gli interessati non incontrano inconvenienti significativi

	PROBABILITÀ	LIVELLO	CRITERIO PROBABILISTICO (PROB. DI ACCADIMENTO STIMATA NELL'ANNO)
VALUTAZIONE DELLA PROBABILITÀ	**4**	Quasi certo	Prob. >50%
	3	Probabile	20% <Prob.< 50%
	2	Moderata	5% <Prob.< 20%
	1	Rara	Prob. <5%

	IMPROBABILE = 1	POSSIBILE (POCO PROB.) = 2	PROBABILE = 3	ALTAMENTE PROBABILE = 4
GRAVI = 4	4	8	12	16
SIGNIFICATIVI = 3	3	6	9	12
MODESTA ENTITÀ = 2	2	4	6	8
LIEVI = 1	1	2	3	4

VALUTAZIONE DEI RISCHI NEL DETTAGLIO ART 35 GDPR

CLASSE RISCHIO	RISCHIO DI DETTAGLIO (POSSONO ESSERE RIPETUTI PER PIÙ CATEGORIE)	FATTORI	PROBABILITA'	IMPATTO/ GRAVITÀ	RISCHIO RESIDUO
RID	utilizzo/accesso di/da dispositivi non inventariati (Pc, Tablet, Smartphone,) anche in lavoro agile	US	2	3	6
RD	predisposizione e attivazione di software/hardware/reti per il controllo degli accessi da remoto (Teamviewer e/o VPN)	US	2	3	6
RID	perdita e/o divulgazione di dato sanitario a seguito dell'obbligo di autodichiarazione dei dipendenti (vedi allegato)	US	1	3	3
RD	replica dei dati su supporto non sicuro/adatto	U	3	3	9
R	installazione di software non autorizzato sulla postazione di lavoro	U	1	3	3
R	divulgazione involontaria delle informazioni (es in un dialogo)	U	2	2	4
R	attacco di ingegneria sociale per carpire informazioni/furto identità	U	2	4	8
R	mancata protezione dei pc (es. schermi non protetti)	U	2	3	6
R	cambio mansione, dimissioni di dipendente	U	2	2	4
R	affidamento di attività di progetto/servizio a fornitori	U	3	2	6
RID	gestione/conservazione dei dati tramite fornitori scelti a supporto della DDI	US	3	3	9
RID	infezioni da virus/malware	S	3	3	9
R	sistema di autenticazione/profilazione/gestione delle credenziali non adeguato	S	3	3	9
RID	errori/vulnerabilità nel software utilizzato	S	2	2	4
R	trasmissioni di dati in maniera non sicura	S	3	3	9
I	installazione di un middleware, software o hw che danneggia i dati	S	1	4	4
RI	comportamenti sleali o fraudolenti di dipendenti	U	2	4	8
ID	errori in fase di aggiornamento dei SO, del middleware, delle configurazioni	US	1	3	3
ID	errori umani involontari di dipendenti (es per poca formazione/competenza, disattenzione, ..)	U	2	4	8
D	evento naturale catastrofico (incendio, inondazione)	C	1	4	4
D	evento vandalico	C	2	2	4
RD	furto di dispositivi (pc, telefono, ipad, hw)	C	2	3	6

D	utilizzo di sw contraffatto/senza licenza	U	1	3	3
D	dimensionamento non corretto dei repository dei dati (DB, file system)	U	1	2	2
D	errori in fase di aggiornamento dei sw applicativo	U	1	3	3
D	scadenza licenza, mancato aggiornamento software	U	1	2	2
D	interruzioni o non disponibilità della rete (guasti)	C	1	3	3
D	indisponibilità del personale (malattia, sciopero, pensionamento, ..)	U	1	2	2
D	furto documenti cartacei	C	2	4	8
D	guasto hardware	S	1	4	4
D	attacchi DOS/DDOS (Distributed Denial of Service)	S	2	4	8
D	interruzioni o non disponibilità dei sistemi complementari (elettricità, climatizzazione, ecc.)	C	1	2	2
RD	archiviazione eseguita in modo incorretto - documenti cartacei NON sensibili	C	2	2	4

R	**Riservatezza**	U	**Comportamento umano**
I	**Integrità**	S	**Eventi relativi agli strumenti**
D	**Disponibilità**	C	**Eventi relativi al contesto**

RISULTATI VALUTAZIONE D'IMPATTO

Di seguito, viene riportata l'analisi di tutte le attività di trattamento per cui si è resa necessaria la valutazione di impatto sulla protezione dei dati.

ALUNNI, GENITORI E/O TUTORI

STRUTTURA e UFFICI COINVOLTI	Amministrazione Ufficio Alunni Segreteria

PERSONALE COINVOLTO	
TITOLARE DEL TRATTAMENTO	Istituto Scolastico nella persona del suo Dirigente scolastico *pro tempore*
PERSONALE INCARICATO	I docenti del Consiglio di classe ed i membri dello staff per l'integrazione scolastica, relativamente ai dati necessari alle attività didattiche, di valutazione, integrative e istituzionali; I collaboratori scolastici ed i componenti degli organi collegiali limitatamente ai dati strettamente necessari allo svolgimento dei propri incarichi; Amministratore di Sistema e assistenti tecnici svolgimento dei loro compiti di assistenza e manutenzione delle strutture informatiche; Personale di segreteria incaricato dell'acquisizione e dell'invio di tutta ladocumentazione istituzionale (Ufficio di Protocollo).
PROCESSO DI TRATTAMENTO	
DESCRIZIONE	Il Titolare tratta i dati personali, identificativi (ad esempio, nome,cognome, CF, telefono, e-mail), "dati personali", "dati sensibili" o anche"dati Giudiziari" da Lei comunicati in sede di iscrizione al ciclo scolastico.
FONTE DEI DATI PERSONALI	Raccolti in sede di iscrizione Ricevuti da Banche Dati di altri Soggetti Pubblici (SIDI, Anagrafe Nazionale degli Studenti) Consenso/autorizzazione

BASE GIURIDICA PER IL TRATTAMENTOPER DATI COMUNI (ART. 6 GDPR)	**INTERESSE LEGITTIMO** Tutti i trattamenti si svolgono esclusivamente al fine di adempiere agli obblighi connessi all'instaurazione ed al mantenimento dei rapporti suddetti per le diverse finalità previste dalle normative vigenti per il funzionamento delle scuole ed ispirandosi ai seguenti principi generali: necessità; liceità; correttezza; lealtà; sicurezza e protezione. Senza pretesa di esaustività (i dettagli saranno contenuti nelle informative specifiche che verranno di volta in volta fornite), i trattamenti svolti dall'Istituto ai sensi dell'art. 6 lettera e) del Regolamento UE sono: iscrizione e frequenza degli allievi; gestione della carriera di personale ed allievi; utilizzo dei servizi telematici e di posta elettronica per tutti i fini; utilizzo di piattaforme a contenuto multimediale per assolvere allo svolgimento della didattica digitale integrata; fruizione di contributi, agevolazioni e servizi connessi ai rapporti intercorrenti con l'Istituto; rilevazioni per la valutazione della didattica; applicazione delle misure di sicurezza degli ambienti di lavoro (D.lgs. 81/2008); gestione dell'offerta formativa e dell'assegnazione degli incarichi; gestione della struttura organizzativa, dell'anagrafica del personale e registrazione degli eventi di carriera (trattamento giuridico del personale); gestione delle pratiche assicurative e previdenziali; trattamenti assistenziali, denunce e pratiche di infortunio, trattamenti assistenziali; attivazione dei protocolli di sicurezza per il contenimento dal rischio contagio da SARS-CoV 2 (misure di screening all'ingresso dei plessi qualora previsti); **CONSENSO/AUTORIZZAZIONE** I Dati personali sono trattati solo previo specifico consenso dell'interessato per taluni procedimenti amministrativi attivabili soltanto su domanda individuale (ottenimento di particolari servizi, prestazione, benefici, esenzioni, certificazioni, ecc.) dove può essere indispensabile il conferimento di ulteriori dati, altrimenti la finalità richiesta non sarebbe raggiungibile
BASE GIURIDICA PER IL TRATTAMENTOPER DATI PARTICOLARI (ART. 9 GDPR)	I dati personali qualificati dal Regolamento UE 2016/679 come sensibili e giudiziari verranno trattati nel rispetto del principio di indispensabilità del trattamento. Di norma non saranno soggetti a diffusione, salvo la necessità di comunicare gli stessi ad altri Enti Pubblici nell'esecuzione di attività istituzionali previste da norme di legge in ambito sanitario, previdenziale, tributario, infortunistico, giudiziario, collocamento lavorativo, nei limiti previsti dal D.M. 305/2006.
FINALITÀ DEL TRATTAMENTO	Obblighi connessi all'instaurazione ed al mantenimento dei rapporti suddetti per le diverse finalità previste dalle normative vigenti per il funzionamento delle scuole
TIPO DI DATI PERSONALI	Personali Dati relativi alla famiglia e a situazioni personali (stato civile, minori, figli, soggetti a carico, consanguinei, altri appartenenti alnucleo familiare) Particolari (sensibili)Giudiziari
CATEGORIE DI INTERESSATI	Alunni Genitori Tutori

	Affidatari
CATEGORIE DI DESTINATARI	Banche dati Ministeriali Soggetti Pubblici (ASL, Comune, Provincia, Ufficio scolastico regionale, Ambiti Territoriali, organi di polizia giudiziaria, organi dipolizia tributaria, guardia di finanza, magistratura) SIDI Altre strutture del sistema della Pubblica Istruzione, altre strutture pubbliche, INAIL, Azienda Sanitaria pubblica competente, Società di Assicurazione per polizza infortuni, Agenzie viaggi (Dati Personali).
INFORMATIVA	Predisposta ad inizio del ciclo scolastico
FREQUENZA TRATTAMENTO	Giornaliera
TERMINE CANCELLAZIONE DATI	I dati personali vengono conservati presso l'Istituto per tutto il tempo in cui la prestazione sarà attiva e verrà trattenuto il fascicolo per il periodo di conservazione obbligatorio previsto dalla normativa vigente. I tempi di conservazione dei dati (senza differenza alcuna tra cartacei e digitali) sono stabiliti dalla normativa di riferimento per le Istituzioni scolastiche individuabile nella Legge 59/1997 (Art. 21), D.P.R. 275/1999, D.P.R. 445/2000, D.Lgs. 42/2004 e Legge 137/2002 (Art. 10).
TRASFERIMENTO DATI (PAESI TERZI)	Previsto a seguito dell'utilizzo di servizi di Cloud computing e piattaforme in uso alla didattica digitale integrata

Categoria dati personali	P*D	R	Livello Rischio
ALUNNO ORDINARIO *Tipo di Dati personali trattati: dati anagrafici, stato civile, soggetti a carico, ISEE, ecc.*	3X1	3	*Modesto*
ALUNNI CON CERTIFICAZIONI *Tipo di Dati personali trattati: Dati sanitari (es. BES, PEI, DVA, DSA, PDP, DISAGI, PATOLOGIE ECC)*	2X4	8	*Rilevante*

PERSONALE ATA e DOCENTI

STRUTTURA e UFFICI COINVOLTI	Amministrazione Ufficio Personale Segreteria

PERSONALE COINVOLTO	
TITOLARE DEL TRATTAMENTO	Istituto Scolastico nella persona del suo Dirigente scolastico *pro tempore*
PERSONALE INCARICATO	Incaricati di segreteria limitatamente all'esercizio delle loro funzioni e ruoli I collaboratori scolastici ed i componenti degli organi collegiali limitatamente ai dati strettamente necessari allo svolgimento dei propri incarichi; Amministratore di Sistema, Aziende o professionisti nello svolgimento dei loro compiti di assistenza e manutenzione delle strutture informatiche; Personale di segreteria incaricato dell'acquisizione e dell'invio di tutta ladocumentazione istituzionale (Ufficio di Protocollo).
PROCESSO DI TRATTAMENTO	
DESCRIZIONE	I dati trattati dall'Istituto scolastico si riferiscono a: dati anagrafici e identificativi (quali ad esempio nominativo, età, luogo e data di nascita, numero di telefono, email, codice fiscale, codice IBAN); informazioni relative alla famiglia (quali ad esempio stato civile, minori a carico, consanguinei, altri appartenenti al nucleo familiare, contatti di emergenza); informazioni relative alla posizione lavorativa (quali ad esempio giorno di assunzione, immissione in ruolo); informazioni relative a istruzione e informazioni professionali e lavorative; Categorie particolari di dati (ai sensi dell'art. 9 e dell'art. 10 del GDPR, quali ad esempio dichiarazioni di infortunio, stato di gravidanza, cartella sanitaria, appartenenza alle categorie protette, partecipazione ad organismi rappresentativi dei lavoratori, casellario giudiziale).
FONTE DEI DATI PERSONALI	Raccolti direttamente Ricevuti da Banche Dati di altri Soggetti Pubblici. Consenso/autorizzazione
BASE GIURIDICA PER IL TRATTAMENTOPER DATI COMUNI (ART. 6 GDPR) e DATI PARTICOLARI (ART. 9 GDPR)	I dati personali e le eventuali variazioni che da Lei comunicate all'Istituto scolastico sono raccolti e trattati per le seguenti ed esclusive finalità: Finalità connesse alla gestione del rapporto di lavoro, basate sull'obbligo legale cui è soggetto il Titolare del trattamento (obblighi contributivi, retributivi, fiscali, di tutela della sicurezza e della salute, di riconoscimento di permessi sindacali, di versamento di trattenute a favore di associazioni sindacali, di gestione della malattia e degli infortuni ed in generale, per tutte le incombenze di spettanza del datore di lavoro, gestione dati per attivazione account piattaforme istituzionali); Finalità ulteriori basate sul consenso dell'interessato (es. riprese foto/audio/video in attività didattiche, convegni o altre attività).
FINALITÀ DEL TRATTAMENTO	Finalità connesse alla gestione del rapporto di lavoro, basate sull'obbligo legale cui è soggetto il Titolare del trattamento

TIPO DI DATI PERSONALI	Personali Particolari (sensibili)Giudiziari
CATEGORIE DI INTERESSATI	Docenti Personale ATA
CATEGORIE DI DESTINATARI	I dati personali in questione potranno essere trasmessi agli Enti previdenziali e assistenziali, all'Amministrazione finanziaria, ai competenti uffici del lavoro e della vigilanza, alle organizzazioni sindacali cui Lei risultasse iscritto, oltre che ai professionisti e fornitori di cui il nostro Istituto si avvale quali RSPP, DPO, medico competente, compagnie di assicurazione, agenzie di viaggio, banche, ed in genere a terzi per i quali si renda necessario nello svolgimento della sua attività lavorativa.
FREQUENZA TRATTAMENTO	Giornaliera
TERMINE CANCELLAZIONE DATI	I dati saranno conservati presso l'Istituto per tutto il tempo in cui la prestazione lavorativa sarà attiva ed in seguito, in caso di trasferimento o pensionamento, verranno inviati alla scuola di destinazione e il Titolare del trattamento provvede all'archiviazione del certificato di prestazione del servizio. previsto dalla normativa vigente. I limiti temporali per la conservazione delle documentazioni degli Archivi sono regolati da una circolare della Direzione Generale per gli Archivi del Ministero per i Beni e le attività, la 28/2008.
TRASFERIMENTO DATI (PAESI TERZI)	Previsto a seguito dell'utilizzo di servizi di Cloud computing e piattaforme in uso alla didattica digitale integrata

CATEGORIA DATI PERSONALI	P*D	R	LIVELLO RISCHIO
DATI di DIPENDENTE ORDINARIO	3X1	3	*Modesto*
DATI di DIPENDENTE ai sensi degli artt. 9 e 10 (ES. DISAGIO, PATOLOGIE, SINDACATI, RELIGIONE, DATI GIUDIZIARI, ECC)	2X4	8	*Rilevante*

FORNITORI ED ESPERTI ESTERNI

STRUTTURA e UFFICI COINVOLTI	Amministrazione Ufficio Acquisti Segreteria

PERSONALE COINVOLTO	
TITOLARE DEL TRATTAMENTO	Istituto Scolastico nella persona del suo Dirigente scolastico *pro tempore*
PERSONALE INCARICATO	Incaricati di segreteria Collaboratori scolastici, limitatamente all'esercizio delle loro funzioni
PROCESSO DI TRATTAMENTO	
DESCRIZIONE	Il Titolare tratta i dati personali, identificativi (ad esempio, nome, cognome, ragione sociale, indirizzo, telefono, e-mail, riferimenti bancari e di pagamento), "dati personali", "dati sensibili" o anche"dati Giudiziari" da Lei comunicati in occasione della conclusione di contratti per i servizi del Titolare.
FONTE DEI DATI PERSONALI	Raccolti direttamente Ricevuti da Banche Dati di altri Soggetti Pubblici.
BASE GIURIDICA PER IL TRATTAMENTOPER DATI COMUNI (ART. 6 GDPR) e DATI PARTICOLARI (ART. 9 GDPR)	Dati anagrafici e di contatto relativi a persone fisiche trattati dalla Società per la stipula e nell'esecuzione del rapporto contrattuale con i Fornitori, ivi inclusi quelli del Fornitore persona fisica, del legale rappresentante del Fornitore persona giuridica (che sottoscrive il contratto in nome e per conto di quest'ultimo), nonché dei dipendenti/consulenti del Fornitore coinvolti nelle attività di cui al contratto.
FINALITÀ DEL TRATTAMENTO	• predisposizione comunicazioni informative precontrattuali e istruttorie rispetto alla stipula di un contratto; • esecuzione del contratto e sua gestione amministrativa: elaborazione, liquidazione e corresponsione degli importi dovuti e relativa contabilizzazione; • analisi del mercato e elaborazioni statistiche; • verifica del grado di soddisfazione dei rapporti; • adempimento di obblighi derivanti da leggi, contratti, regolamenti in materia di igiene e • sicurezza del lavoro, in materia fiscale, in materia assicurativa; • tutela dei diritti in sede giudiziaria.

TIPO DI DATI PERSONALI	Dati personali in genere
CATEGORIE DI INTERESSATI	Fornitori di prodotti e/o servizi Esperti esterni Tirocinanti universitari

CATEGORIE DI DESTINATARI	I soggetti a cui i dati personali potranno essere comunicati nell'ambito della scuola sono: il Dirigente Scolastico, gli incaricati con codici di amministratore (D.S.G.A., Collaboratore Vicario e Animatore Digitale), gli Incaricati del trattamento amministrativo (che di fatto corrispondono a tutto il personale). I dati personali, diversi da quelli sensibili e giudiziari, potranno essere comunicati ad altri enti pubblici o privati esclusivamente nei casi previsti da leggi e regolamenti (per esempio: altre strutture del sistema della Pubblica Istruzione, altre strutture pubbliche, INAIL, ASL competente, Softwarehouse, Comune, Provincia, USR, ATP, Guardia di finanza, ed altri).
FREQUENZA TRATTAMENTO	Giornaliera
TERMINE CANCELLAZIONE DATI	I dati personali raccolti per le finalità indicate al punto 3 saranno conservati per tutta la durata del contratto e, dopo la cessazione, per al più 10 anni. Nel caso di contenzioso giudiziale, i Dati saranno conservati per tutta la durata dello stesso, fino all'esaurimento dei termini di esperibilità delle azioni di impugnazione.
TRASFERIMENTO DATI (PAESI TERZI)	Non previsto

Categoria dati personali	P*D	R	Livello Rischio
DATI ANAGRAFICI	2X1	2	*Modesto*
DATI PARTICOLARI (AUTODICHIARAZIONE ai sensi dell'art. 10 GDPR 679/16 e dell'art. 46, 47 e 76 e ss. del D.p.r. 445/2000, TRACCIABILITA' DEI FLUSSI, ECC...)	2X4	8	*Rilevante*

MODALITA' DI ELABORAZIONE DATI: ELETTRONICA E CARTACEA

STRUMENTI	Registro Elettronico Segreteria Digitale Piattaforme in Cloud Piattaforme ministeriali

STRUTTURE INFORMATICHE DI ARCHIVIAZIONE

SERVER	Struttura interna Esterno (softwarehouse)	
Sede di riferimento	Sede amministrazione	
Personale con diritti di accesso	Personale incaricato e tecnici informatici interni ed esterni (qualora nominati)	
SOFTWARE UTILIZZATI	Java Kasperskay Adobe Reader DC Google Chrome Mozilla Firefox	Software Gestionale: Argo WinRar Microsoft Office Libre Office
SOFTWAREHOUSE		
REGISTRO ELETTRONICO	NUVOLA-MADISOFT	
SEGRETERIA DIGITALE – PROTOCOLLO	NUVOLA-MADISOFT	
ANAGRAFICA, PERSONALE	ARGO	
PAGAMENTI, BILANCIO	ARGO	
SITO WEB	KARON	

STRUTTURE INFORMATICHE DI BACKUP

NAS	
Sede di riferimento	Plesso principale
Frequenza di backup	Giornaliera
Rotazione HDD	-
Personale con diritti di accesso	Incaricati interni e BE TECH S.A.S. DI BETTOSCHI G. & BONACINA L.
Software utilizzati	-
Custodia copie di Backup	-
CLOUD	
NUVOLA-MADISOFT, ARGO	
SERVER	
Il Server è presente appunto nella sala SERVER in un armadio chiuso a chiave	

VALUTAZIONE ADEGUATEZZA DELLE MISURE DI SICUREZZA ADOTTATE (versione sintetica)

DATI DIGITALI/INFORMATICI

L'Istituto sta implementando le misure di sicurezza obbligatorie del Regolamento UE (art. 32 e ss.), e le misure minime Agid - ICT (Es. credenziali d'accesso controllate; politica di Backup; presenza di un Firewall con log di accessi; cablaggio della rete con sottoreti univoche; Gruppo di continuità presente; Politica password; ecc.). 2. Le nomine ad incaricati sono state trascritte. 3. i dati conservati sui PC interni all'Istituto sono protetti da accesso controllato, limitato ai compiti della funzione di riferimento. 4. l'Istituto si è dotato di una politica scritta di backup. 5. l'accesso all'Istituto è controllato. 6. Il sistema informativo dell'ente risponde alle indicazioni fornite da AGiD per le misure minime di sicurezza ICT. I dati memorizzati su supporto informatico sono gestiti all'interno di tale sistema. I dati riportati su documentazione e registri cartacei seguono le procedure indicate nel manuale di gestione del protocollo cartaceo. Se il trattamento è svolto in parte o nella sua interezza da un responsabile esterno, l'Istituto delega tale organizzazione tramite un atto specifico alla sicurezza e alla protezione dei dati.

DDI & SMARTWORKING

L'Organizzazione ha predisposto politiche di controllo all'utilizzo di soli servizi e strumenti autorizzati a supporto della Didattica Digitale Integrata. L'Organizzazione assicura, inoltre, l'adozione di misure di sicurezza adeguate dei propri dipendenti/collaboratori finalizzate alla riservatezza dei dati trattati e della custodia degli strumenti messi a disposizione dal Titolare del Trattamento. A tal proposito l'Organizzazione provvede alla regolare formazione dei propri lavoratori per renderli edotti circa le misure di prevenzione predisposte per fronteggiare rischi connessi all'esecuzione della prestazione da remoto e mediante l'utilizzo di dispositivi personali.

DATI CARTACEI

L'Organizzazione conserva i "dati particolari" dell'utenza interessata (ALUNNI/GENITORI, FORNITORI ed ESPERTI ESTERNI, PERSONALE SCOLASTICO in armadi chiusi a chiave nella Segreteria organizzativa, in particolare sotto chiave o in busta chiusa. Per consultare il proprio fascicolo, l'interessato compila l'apposita richiesta d'accesso, convalidata dal Titolare del Trattamento; l'atto della consultazione avviene sotto supervisione. La sede amministrativa dell'Istituto è protetta da allarme e da vigilanza notturna.

ANALISI PRELIMINARE e VALUTAZIONE DI IMPATTO SOFTWAREHOUSE & DDI

TIPOLOGIA	"REGISTRO ELETTRONICO/		PIATTAFORMA MULTIMEDIALE	
FORNITORE	NUVOLA-MADISOFT		MICROSOFT OFFICE 365	
INDIRIZZO/SEDE	ITALIA		WASHINGTON	
Livello di conoscenza e di usabilità c/o famiglie alunni (Peso max 16,66%)	ALTO		ALTO	
	MEDIO	X	MEDIO	X
	BASSO		BASSO	
Livello di conoscenza c/o docenti (Peso max 16,66%)	ALTO	X	ALTO	
	MEDIO		MEDIO	X
	BASSO		BASSO	
Livello di efficacia/ efficienza piattaforma (metodologia didattica) (Peso max 16,66%)	ALTO	X	ALTO	X
	MEDIO		MEDIO	
	BASSO		BASSO	
Livello di efficacia/ efficienza piattaforma (caratteristiche tecniche) (Peso max 16,66%)	ALTO	X	ALTO	X
	MEDIO		MEDIO	
	BASSO		BASSO	
Livello delle modalità di gestione della piattaforma (Peso max 16,66%)	ALTO		ALTO	
	MEDIO	X	MEDIO	X
	BASSO		BASSO	
Livello di sicurezza informatica e protezione privacy della piattaforma (Peso max 16,66%)	ALTO	X	ALTO	X
	MEDIO		MEDIO	
	BASSO		BASSO	
RISULTATO in %	88,9%		83,3%	

CONCLUSIONI: le piattaforme sottoposte ad analisi sono state scelte sulla base delle indicazioni presenti sul sito del Ministero dell'Istruzione e delle conoscenze esistenti all'interno dell'Istituto. Sulla base delle valutazioni effettuate tenendo conto del parere dello staff dirigenziale, dello staff degli animatori digitali e del Consiglio d'Istituto, si decide di adottare per la DDI: il registro elettronico "NUVOLA" con tutte le sue applicazioni interne (assegno compiti, restituzione compiti, segnalazioni link, agenda, scambio di file, videoconferenza integrata ecc), ed in alternativa gli applicativi di MICROSOFT OFFICE 365. Per le videolezioni si possono utilizzare entrambi i portali effettuando i collegamenti sia dal registro elettronico che dell'apposita area delle videolezioni.

LEGENDA	**ROSSO** (VPF < 60%) SCONSIGLIATO. DA UTILIZZARE SOLO IN CASI PARTICOLARI E CON AUTORIZZAZIONE DEL DS	**GIALLO** (60% ≤ VPF ≤ 75%) DA UTILIZZARE PER PRESTAZIONI SPECIFICHE	**VERDE** (VPF >75%) CONSIGLIATO

VALUTAZIONE ADEGUATEZZA DELLE MISURE DI SICUREZZA ADOTTATE

Allegato "Misure di sicurezza" e di "Garanzia" di cui all'articolo 32 e ss. del GDPR e all'art. 2 septies del D. Lgs. n. 196/03, così come modificato dal D. lgs. n. 101/18

SCOPO

In questa sezione sono riportate, in forma sintetica e schematica, ***le misure in essere e da adottare per contrastare i rischi individuati.*** *Per misura si intende lo specifico intervento tecnico od organizzativo posto in essere per prevenire, contrastare o ridurre gli effetti relativi ad una specifica minaccia, come pure quelle attività di verifica e controllo nel tempo, essenziali per assicurarne l'efficacia.*

*Secondo la definizione ISO, la sicurezza è "****l'insieme delle misure atte a garantire la disponibilità, l'integrità e la riservatezza delle informazioni gestite****" e dunque l'insieme di tutte le misure atte a difendere il sistema informatico dalle possibili minacce d'attacco.*
Rendere sicuro un sistema informatico non significa esclusivamente attivare un insieme di contromisure specifiche, di carattere tecnologico ed organizzativo, che neutralizzino tutti gli attacchi ipotizzabili al sistema di servizi, ma significa, in particolare, collocare ciascuna delle contromisure individuate in una politica organica di sicurezza, che tenga conto dei vincoli (tecnici, logistici, organizzativi, amministrativi e legislativi) imposti dalla struttura tecnica ed organizzativa, in cui il sistema di servizi opera e che giustifichi ciascuna contromisura in un quadro complessivo.
Principale obiettivo di un sistema di sicurezza è la salvaguardia delle informazioni.
Si individuano ***tre*** *aspetti fondamentali relativi alla sicurezza delle informazioni:*

- ***Confidenzialità:*** *solo gli utenti autorizzati possono accedere alle informazioni necessarie;*
- ***Integrità****: protezione contro alterazioni o danneggiamenti, tutela dell'accuratezza e completezza dei dati;*
- ***Disponibilità:*** *le informazioni sono rese disponibili quando occorre e nell'ambito di un contesto pertinente.*

L'approccio alla sicurezza deve avvenire in una logica di prevenzione (risk assessment) piuttosto che in una logica di gestione delle emergenze o di semplice controllo/vigilanza.

L'architettura per rispondere alle esigenze di sicurezza è costituita da 3 elementi fondamentali:

a) le politiche dell'organizzazione;
b) gli strumenti organizzativi e tecnologici;
c) gli atteggiamenti individuali.

Un sistema di gestione della sicurezza delle informazioni efficiente ed efficace permette all'organizzazione di:

a) mantenersi aggiornata su nuove minacce e vulnerabilità e prenderle in considerazione in modo sistematico;
b) trattare incidenti e perdite in ottica di prevenzione e di miglioramento continuo del sistema;
c) sapere quando politiche di sicurezza e procedure non sono implementate, in tempo utile per prevenire danni;
d) implementare politiche e procedure di primaria importanza.

LE DIMENSIONI DELLE ANALISI

Le Misure di sicurezza che l'Istituto adotta sono state scelte con riferimento a criteri e procedure fisiche, logiche, organizzative e tecniche, in grado di assicurare:

a) la protezione delle aree e dei locali in cui sono conservati i dati;
b) il controllo sull'accesso nei predetti locali delle persone autorizzate;
c) l'integrità dei dati;
d) la trasmissione dei dati, ivi comprese le misure di sicurezza da adottarsi per le restrizioni di accesso per via telematica.

***L'obiettivo è esplicitare lo stato dell'arte dell'Istituto in termini di copertura rispetto ai requisiti minimi ed idonei delle misure di sicurezza previste dalla Legge**, come dettagliato nei paragrafi successivi.*

MISURE DI SICUREZZA - ARCHIVI CARTACEI

TIPO	*MISURE DI SICUREZZA*	*STATO*	*RACCOMANDAZIONI e NOTE*
ADEGUATA	***Descrizione dei Locali, con particolar attenzione nell'aver cura** degli atti e dei documenti contenenti dati personali*	*C.*	Ufficio personale - Ufficio contabilità - Ufficio acquisti Ufficio didattica - Ufficio affari generali Ufficio DSGA
ADEGUATA	*Procedere **all'archiviazione dei dati dopo l'uso** negli appositi spazi messi a disposizione dall'organizzazione*	*C.*	*Tutti gli incaricati hanno ricevuto una **formazione** dedicata in materia di Protezione dei dati personali. Da programmare corsi di formazione per personale di nuova presa di servizio.*
ADEGUATA	***Divieto di lasciar documenti incustoditi**, anche per brevi periodi, trasmetterli o consegnarli a terzi senza preventiva specifica autorizzazione*	*C.*	*Tutti gli incaricati hanno ricevuto una **formazione** dedicata in materia di Protezione dei dati personali. Da programmare corsi di formazione per personale di nuova presa di servizio.*
ADEGUATA	***Divieto di divulgare** all'esterno il contenuto degli stessi archivi.*	*C.*	*Tutti gli incaricati hanno ricevuto una **formazione** dedicata in materia di Protezione dei dati personali. Da programmare corsi di formazione per personale di nuova presa di servizio.*

ADEGUATA	***Identificare e registrare le persone ammesse** a qualunque titolo dopo gli orari di chiusura degli uffici.*	*C.*	*Nessuno è autorizzato ad entrare nell'Istituto dopo l'orario di chiusura.*
ADEGUATA	***Conservazione** dei documenti cartacei.*	*C.*	*FASCICOLI DEL PERSONALE: nell'ufficio del personale gli armadi sono chiusi a chiave ogni sera.* *FASCICOLI DEGLI ALUNNI: nell'ufficio didattica gli armadi sono chiusi a chiave ogni sera.* *FASCICOLI DEI FORNITORI: nell'ufficio acquisti gli armadi sono chiusi a chiave ogni sera*

MISURE DI SICUREZZA - ARCHIVI CARTACEI

ADEGUATA	*Controllare periodicamente gli archivi, procedendo alla **distruzione** dei dati non più necessari e/o dei dati per i quali risulta terminato il periodo di conservazione indicato dal TITOLARE, in modo controllato e documentato*	*C.*	

GESTIONE E CONTROLLO DEGLI ACCESSI AI SISTEMI (es. Softwarehouse)

TIPO	***MISURE DI SICUREZZA***	***STATO***	***RACCOMANDAZIONI e NOTE***
ADEGUATA	*Codice identificativo associato ad una Password per l'accesso ai PC.*	*C.*	
ADEGUATA	***Assegnare singoli terminali e/o utenze nominali**, prevedendo deroghe solo ove strettamente necessario e limitatamente a specifiche funzioni*	*C.*	
ADEGUATA	*Password di **almeno 8 caratteri** alfanumerici.*	*C.*	*Tutti i computer utilizzati possiedono una password conforme. Il Login viene dato all'atto dell'assunzione.*
ADEGUATA	***Periodica modifica** dei Codici identificativi associati ad una PSW per l'accesso ai PC.*	*C.*	*Le password devono essere modificate almeno ogni 6 mesi (ogni 3 mesi in caso di trattamento di dati sensibili o particolari).*
ADEGUATA	***Profilazione** – Codice identificativo associato ad una PSW per l'accesso al gestionale*	*C.*	*Ogni dipendente ha un proprio login di accesso personalizzato.*
ADEGUATA	*Definire e pubblicare **regole** per la gestione delle utenze e dei profili di accesso e operativi*	*C.*	*Regole disponibili tramite mansionario*
ADEGUATA	*Fornire precise **istruzioni** ai propri dipendenti e collaboratori sulle modalità con cui i dati personali del Titolare dovranno essere trattati*	*C.*	*Istruzioni disponibili nel Sistema di Gestione. Si raccomanda la pubblicazione mediante affissione delle politiche operative di gestione dei dati nei locali di segreteria.*
ADEGUATA	***Identificazione** del terminale e/o dell'utente che accede ai sistemi.*	*C.*	*Profilazione e credenziali di accesso univoche*

ADEGUATA	***Sospensione automatica** del terminale lasciato inattivo, con la necessità di inserire identificazione utente e password per riavviarlo*	*C.*	*Misura implementata* *Misura da implementare*
ADEGUATA	***Blocco automatico dell'identificazione utente in caso di errato inserimento della password** e/o dell'utenza e tracciamento dei tentativi di accesso effettuati*	*C.*	*Misura implementata* *Misura da implementare*
ADEGUATA	*Definizione, per ciascun utente, di un **profilo di accesso ai dati personali adeguato al ruolo** a questi assegnato e limitatamente ai soli diritti necessari per le fasi dell'elaborazione*	*C.*	*Credenziali di accesso univoche*

MISURE DI SICUREZZA LOGICHE – PROTEZIONE DATI INFORMATICI

TIPO	MISURE DI SICUREZZA	STATO	RACCOMANDAZIONI e NOTE
ADEGUATA	*Utilizzo di programmi **ANTIVIRUS**.*	*C.*	*Kaspersky Antivirus su tutti i terminali*
ADEGUATA	*Aggiornamento programma ANTIVIRUS.*	*C.*	*Aggiornamento automatico*
ADEGUATA	***Sistemi operativi** aggiornati nei PC in uso.*	*C.*	*Sono presenti PC con windows 10 che riceve aggiornamenti*
ADEGUATA	*Utilizzo di programmi **FIREWALL**.*	*C.*	*Sophos. Il Firewall viene aggiornato in automatico.*
ADEGUATA	*Aggiornamento programma FIREWALL.*	*C.*	*Firewall con hardware dedicato.*
ADEGUATA	***Registrazione, monitoraggio, e tracciamento degli accessi** al data center dove sono conservati i dati personali.*	*C.*	*Tramite firewall.*
ADEGUATA	***Divieto di accesso a siti** Internet non autorizzati. (Filtri siti web)*	*C.*	*Tramite firewall.*
ADEGUATA	***Monitorare** i soggetti autorizzati a cancellare e/o modificare i dati personali*	*C.*	
ADEGUATA	*BACK-UP (almeno settimanale) dei Dati.*	*?*	*Il back-up avviene giornalmente in maniera automatica:* *- su ogni server (compreso il gestionale): Cartelle condivise e database.* *- Fisico su NAS/HDD*
ADEGUATA	***Conservare** i BACK-UP in un luogo sicuro (in un contenitore ignifugo) o in Cloud*	*?*	
ADEGUATA	***Verificare** i BACK-UP almeno ogni 15 giorni per il controllo di integrità e leggibilità dei supporti*	*C.*	*I Back up vengono controllati regolarmente.*

ADEGUATA	***Sala server** con adeguate condizioni di uso e di archivio*	*N.C.*	*Sala server chiusa a chiave. Apposito armadio rack presente. Impianto di condizionamento presente*
ADEGUATA	*Gruppo di continuità elettrica.*	*P.*	

MISURE DI SICUREZZA ORGANIZZATIVE

TIPO	***MISURE DI SICUREZZA***	***STATO***	***RACCOMANDAZIONI e NOTE***
ADEGUATA	*E' prevista la **pseudonimizzazione/ anonimizzazione** e la cifratura dei dati personali?*	*N.C.*	*Si stanno implementando le procedure di **pseudonimizzazione** e di cifratura attraverso programmi appositi (es. PEI; PDP, Allegati email, Sito web HTTPS,).*
ADEGUATA	*E' prevista la capacità di **assicurare su base permanente la riservatezza, l'integrità, la disponibilità** e la resilienza dei sistemi e dei servizi di trattamento?*	*C.*	*Vedi allegato misure di sicurezza ex. Art. 32 e ss. del GDPR.* *In particolare:* - ***Relazione del DPO**.*
ADEGUATA	*E' prevista la capacità di **ripristinare tempestivamente la disponibilità** e l'accesso dei dati personali in caso di incidente fisico o tecnico?*	*C.*	*In loco è presente un dispositivo NAS con funzione di Back up, oltre al salvataggio dei dati da parte del server. Vedi la politica allegata al MSG (Manuale di Sistema di Gestione privacy) – Incidenti: dall'incidente al post-risoluzione.*
ADEGUATA	***Disattivazione del codice** (e di eventuali altre password e credenziali) in caso di cambiamento/termine della mansione.*	*C.*	*Avviene a carico del Personale incaricato.*
ADEGUATA	*È prevista una **procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche** e organizzative al fine di garantire la sicurezza del trattamento?*	*N.C.*	*Si consiglia di prevedere con il consulente informatico un esame di **Vulnerability Assessment**, (da implementare) a cadenza ciclica.*
ADEGUATA	***Divieto** di utilizzo di Software non approvato.*	*P.*	*Sia per la segreteria che per la didattica non è possibile per l'utente. Solo l'amministratore può installare programmi.*
ADEGUATA	*Controlli sul tipo di SOFTWARE installato al fine di rilevare quelli non appropriati.*	*P.*	*Autorizzazioni e controlli effettuate dall'amministratore di rete.*
ADEGUATA	*Softwarehouse in Cloud*	*C.*	*NUVOLA-MADISOFT, ARGO; RARON (sito web)*
ADEGUATA	*Piattaforme multimediale*	*C.*	*MICROSOFT OFFICE 365 FOR EDU; GOOGLE WORKSPACE*

MISURE DI SICUREZZA per il SITO WEB

TIPO	MISURE DI SICUREZZA	STATO	RACCOMANDAZIONI e NOTE
ADEGUATA	L'Istituzione possiede un sito Web con dominio personale?	C.	https://iccapriolo.edu.it/
ADEGUATA	E' stata effettuata la nomina come **Responsabile esterno** del trattamento alla società esterna che gestisce il sito?	C.	KARON
ADEGUATA	È stata predisposta **l'informativa** (facendo riferimento eventualmente anche all'area riservata) sul Sito Web tramite link apposito?	N.C.	Da sostituire con modelli aggiornati
ADEGUATA	È stato raccolto il **consenso** dagli interessati qualora nel Sito Web fossero pubblicati foto/audio/video?	C.	Ottenuto ad inizio del ciclo scolastico. Predisporre nuovi modelli di Privacy Control per le prossime iscrizioni
ADEGUATA	Sono state **predisposte le 3 informative privacy** (alunni/famiglie, dip.e fornitori) nella sez. privacy?	C.	Da inserire modelli predisposti da Privacy Control
ADEGUATA	Il **DPO** è stato pubblicizzato nella sez. privacy?	N.C.	Dati da aggiornare a seguito di nuovo incarico
ADEGUATA	Sono stati predisposti i banner per i **cookies** obbligatori nel sito web?	C.	Cookie banner e cookie policy presenti
ADEGUATA	È presente un Cookie banner con flag di spunta per eventuali cookie analitici e/o di profilazione? È presente una Cookie policy?	C.	Cookie banner e cookie policy presenti
ADEGUATA	È presente la dichiarazione di accessibilità al sito web secondo indicazioni AgID?	N.C.	Dichiarazione di accessibilità: non presente
ADEGUATA	Sono stati pubblicati gli Obiettivi di accessibilità?	C.	Presenti 2022
ADEGUATA	È stato pubblicato in Amministrazione trasparente il Manuale di gestione dei flussi documentali con i relativi allegati?	P.	Documenti mancanti

MISURE DI SICUREZZA FISICHE

TIPO	MISURE DI SICUREZZA	STATO	RACCOMANDAZIONI e NOTE
ADEGUATA	Accesso selezionato e controllato.	C.	La porta di accesso è gestita attraverso un ingresso controllato da un front office dedicato.
ADEGUATA	Definizione e delimitazione di aree di sicurezza.	C.	DVR presente
ADEGUATA	Messa in sicurezza delle **attrezzature decentralizzate** per il	C.	

	trattamento dei dati personali, tra cui anche personal computer, laptop, tablet, smartphone, etc.		
ADEGUATA	*Vigilanza esterna.*	*N.P.*	
ADEGUATA	*Impianto di videosorveglianza*	*N.P.*	
ADEGUATA	*Dispositivi di allarme.*	*P.*	*Attivazione e disattivazione manuale. Presente impianto di allarme con collegamento esterno.*
ADEGUATA	*Chiavi di accesso*	*C.*	*Le chiavi di accesso sono consegnate al personale incaricato.*
ADEGUATA	*Sistema antincendio.*	*P.*	

LEGENDA:	
C.: CONFORME	N.C.: NON CONFORME *(ADEGUATEZZA OBBLIGATORIA)*
P.: PRESENTE	N.P.: NON PRESENTE *(ADEGUATEZZA SUFFICIENTE)*